(2)

ESD-TR-88-271

MTR-10373

Computer Security Products Technology Overview

By

T. J. Bergendahl
K. S. Smith
J. G. Sullivan

October 1988

Prepared for

Deputy Commander for Advanced Decisions Systems
Electronic Systems Division
Air Force Systems Command
United States Air Force
Hanscom Air Force Base, Massachusetts

Approved for public release;
distribution unlimited.

Project No. 4610

Prepared by

The MITRE Corporation
Bedford, Massachusetts

Contract No. F19628-86-C-0001

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution unlimited.
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) MTR-10373 ESD-TR-88-271	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION The MITRE Corporation 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) Burlington Road Bedford, MA 01730	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING / SPONSORING ORGANIZATION Deputy Commander (continued) 8b. OFFICE SYMBOL (If applicable) ESD/XRSI	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER F19628-86-C-0001
8c. ADDRESS (City, State, and ZIP Code) Electronic Systems Division, AFSC Hanscom AFB, MA 01731-5000	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. 4610 / TASK NO / WORK UNIT ACCESSION NO.
11. TITLE (Include Security Classification) Computer Security Products Technology Overview	
12. PERSONAL AUTHOR(S) Bergendahl, T. J., Smith, K. S., Sullivan, J. G.	
13a. TYPE OF REPORT Final 13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Year, Month, Day) 1988 October 15. PAGE COUNT 50
16. SUPPLEMENTARY NOTATION	
17. COSATI CODES FIELD / GROUP / SUB-GROUP	18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) Computer Security Products COTS Products (continued)

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

This paper provides an overview of currently available computer security techniques and was written in support of the Security Products Program (SecurityPro). The program was established under the ESD Computer Resource Management Technology Program (PE64740F) in response to the SAC Statement of Need (SON) 10-82. The SecurityPro program is an attempt to identify and address SAC's specific computer security needs.

Keywords: [illegible] host, data base [illegible] (KR)

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL Pamela J. Cunha	22b. TELEPHONE (Include Area Code) (617) 271-2844 22c. OFFICE SYMBOL Mail Stop D135

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

8a. for Advanced Decisions Systems

18. EPL
Evaluated Products
Multi-User Hosts
SAC SON 10-82

ACKNOWLEDGMENT

This document has been prepared by The MITRE Corporation under Project No. 4610, Contract No. F19628-86-C-0001. The contract is sponsored by the Electronic Systems Division, Air Force Systems Command, United States Air Force, Hanscom Air Force Base, Massachusetts 01731-5000.

TABLE OF CONTENTS

TABLE OF CONTENTS (Concluded)

SECTION 1

INTRODUCTION

This overview is written in support of the Security Products Program in response to the Strategic Air Command (SAC) SON 10-82. The program effort focuses on identifying specific computer security needs at SAC which may be met with products that significantly improve computer security. This paper focuses on currently available products and on technological trends that would be useful in the SAC environment.

SAC has operational needs to process large volumes of data, to transfer data between intelligence and collateral communities, to produce reports on an *ad hoc* as well as a routine basis, and to facilitate rapid communication among the various SAC communities.

The types of computer security systems this paper addresses fall into the areas of multi-user hosts, database management systems (DBMS), workstations, networks, guards and gateways, and miscellaneous computer security products. A heavy emphasis is on products that have been evaluated by the National Computer Security Center (NCSC), because SAC must comply with DOD (the Joint Chiefs of Staff (JCS) and the Defense Intelligence Ageny (DIA) as well as Air Force) policy, and that policy encourages the use of such products.

NEED FOR MULTILEVEL COMPUTER SECURITY

Security in computer systems is met by a combination of physical, operational, procedural, communication, and hardware/software safeguards. Physical, operational, and procedural safeguards are well understood, and can be used to compensate for the lack of computer security. Reliance on controls external to the computers, however, becomes increasingly restrictive with the growth of the power and capability of computers. Much of the power of information systems comes from the ability to interconnect systems and reliably exchange information between those systems at high data rates. The relatively recent requirement within the DOD for adaptive planning, at any level, requires the use of exactly this kind of flexible computing power and capability.

DOD needs to reflect its complex classification structure in the computer systems used to process classified information. The classification structure includes hierarchical levels from Unclassified to Top Secret and non-hierarchical levels, including compartments and handling caveats. The need to exchange

information securely between classification levels and to combine information securely across categories and handling caveats while at the same time maintaining information at its appropriate classification level is another driving force in computer security.

DOD Directive 5200.28 "Security Requirements for ADP Systems," [1] defines DOD policy for protection of classified information stored in or processed by a computer. Security safeguards include physical and procedural safeguards such as locked doors, armed guards, personnel clearance requirements, file backup procedures, and disaster planning. The regulation also allows for the use of technology to provide a portion of that protection, for example, a password scheme, a file protection mechanism, a secure database management system, or even a fingerprint scanner for user authentication.

Another reason for improved computer security is the DOD need to exchange information with the private sector, as with satellite tracking, and the strong DOD interest in fostering the exchange of ideas among the DOD, the private sector, and academic communities, as, for example, with Arpanet.

This paper focuses on the technological means of providing computer security protection which could improve or replace many current physical and procedural safeguards, thus reducing costs and expanding computing capabilities.

NATIONAL COMPUTER SECURITY CENTER

In 1978 the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence established the Department of Defense Computer Security Initiative to achieve the availability of trusted computer systems for Federal Government use. In January 1981 the DOD Computer Security Evaluation Center was established. The Center was chartered with providing policy, assigning responsibilities for the technical evaluation of computer system and network security, and related technical research [2]. In 1985 the responsibilities of the Center were expanded to include Federal computer security, and the Computer Security Evaluation Center was renamed to the National Computer Security Center (NCSC).

TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

The "Trusted Computer System Evaluation Criteria (TCSEC)," [3] is a DOD Standard issued by the National Computer Security Center which provides a basis for the evaluation of the effectiveness of security controls built into a commercial computer system. The degree of trust that can be placed in a computer

processing classified information can then be assessed and compared with other systems.

The TCSEC is divided into four hierarchical evaluation divisions, D, C, B, and A, with Division A being the most trustworthy. Within divisions C, B, and A are numbered classes (C1, C2, B1, B2, B3, A1); the higher the number, the greater the trust. Within each C, B, and A class, four requirements are stated that must be satisfied: the security policy that is enforced; the accountability of a user to specific actions; the assurance that the system is operating according to its stated security policy; and the documentation that must be provided. The divisions represent major differences in the ability of a system to meet security requirements, and the classes represent incremental improvements.

Brief comments relating to each division follow.

Division D is reserved for systems that have been evaluated, but which fail to meet the requirements for a higher evaluation class.

Division C systems provide need-to-know protection, and, with audit capabilities, provide accountability of subjects and their actions.

Division B systems preserve the integrity of sensitivity labels by using a Trusted Computing Base (TCB). These labels are used to enforce a set of mandatory access control rules. The security policy model that the TCB is based on must be provided by the developer, and evidence must be provided to demonstrate that the reference monitor concept has been implemented.

Division A systems are characterized as having had their mandatory and discretionary security controls formally verified. In addition, extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development, and implementation.

Interpretations of the TCSEC for networks and for databases are currently under development by the NCSC. The "Trusted Network Interpretation (TNI)," [4], released in July 1987, will be used to evaluate networks and network components.

THE EVALUATED PRODUCTS LIST (EPL)

An evaluated product is a commercial product that has been through the NCSC's evaluation process successfully. The product is given a TCSEC evaluation class rating and placed on the NCSC's Evaluated Products List. The evaluation process was set up to encourage the development of secure systems in

the commercial world. Its success is demonstrated by the waiting period now encountered by the many vendors of secure computer products.

CERTIFICATION AND ACCREDITATION

After a product has been evaluated, it must be certified and accredited before it can be used in an operational environment.

Certification is the analysis of an application system against its security requirements. A certification is required for several separate areas, including physical security, personnel security, communications security (COMSEC), computer security (COMPUSEC), emanations security (TEMPEST), and administrative security.

A COMPUSEC certification is a technical analysis of a specialized system in a particular environment to determine the degree to which it meets security requirements. COMPUSEC certifications can be performed by many different organizations within DOD, and although NSA is usually asked to perform certifications for critical systems, it frequently must refuse to do so for lack of resources. The TCSEC can be interpreted as providing the basis of the COMPUSEC requirements.

A system must be accredited before it becomes operational. This task is performed by a designated approving authority (DAA). The DAA assesses the threats, the risks, and the certification results before making a decision to allow the system to operate in a specific environment.

ENVIRONMENTS GUIDELINES

NCSC has published guidelines, referred to as "Environments Guidelines," to assist certifiers and accreditors in determining what TCSEC class is required in a given environment [5]. These guidelines recommend the minimum evaluation class that is needed for a specific environment based on a simple risk index. The risk index is based on the difference between the clearance held by the least-cleared person and the most sensitive data in the system. Appropriate minimum evaluation classes are then assigned according to whether the application system is developed and maintained in an open or closed environment.

VENDORS

Numerous vendors are cited throughout this paper, and selected vendor addresses are listed in Appendix A.

Information relating to computer security products currently under evaluation by the NCSC was obtained directly from vendor sources.

SECTION 2

MULTI-USER HOSTS

DEFINITION

Multi-user hosts can support more than one user at a time. They are general-purpose machines that are usually used for tasks such as office automation, database management, graphics display processing, or near-real-time scientific applications.

ISSUES

The term multi-user host deliberately puts no limitation on the size or power of the machine. Security concerns have much more to do with the way in which a system is used than with the performance of the machines doing the work. The number of simultaneous users of a system, who they are, and the kind of physical and logical access they have to a system substantially defines the technical problems to be solved in protecting sensitive information.

STANDARDS AND GUIDELINES

The TCSEC is used by NCSC to evaluate the operating systems of multi-user hosts. The TCSEC is also used to provide the basis for defining security requirements and evaluating the applications which run on these systems. The Environments Guideline [5] is used to determine what class of system is needed given an operational environment, the levels of the data, and the clearances of the users.

CURRENTLY AVAILABLE SYSTEMS

Security techniques currently available in host computers are largely reflected in the NCSC's Evaluated Product List (EPL). A summary of the secure operating systems on the EPL follows. In each case the overall evaluation class is given and the product description as it appears on the EPL follows in indented format. Comments relating to each system are also provided.

Secure Communications Processor (SCOMP), STOP Release 2.1: The SCOMP has been assigned an overall evaluation class of **A1**.

> The SCOMP hardware consists of a standard HONEYWELL Level 6/DPS 6 16-bit minicomputer with a modified Central Processing Unit (CPU), to which a Security Protection Module (SPM) has been added. The SPM provides segmentation, paging, and protection rings similar to the HONEYWELL Level 68 Multics, with argument validation, and virtual address translation. The virtual environment includes virtual I/O as well as virtual memory.
>
> The primary software security mechanism of the SCOMP system is the security kernel, based on the Center-approved Bell-LaPadula model of the DOD security policy. The security kernel functions as the software portion of the reference monitor implementation. As such, it controls access to objects in accordance with its embedded security policy. The security kernel supports both mandatory and discretionary controls, and provides a strong foundation on which to build secure applications programs.
>
> The Trusted Software (a set of security-relevant, non-kernel code) provides a basic terminal-oriented operating system interface that runs on, and derives its security from, the security kernel and the SCOMP system architecture. There are three categories of Trusted Software. Trusted user services provide the interface to the SCOMP system for the user, trusted operation services provide the system operator with the capabilities necessary to run the system, and trusted maintenance services allow the system administrator to build and maintain the SCOMP system [6].

SCOMP software is supported by Honeywell Federal Systems Division in McLean, VA, and the hardware is supported by Honeywell Custom and Special Products Operation in Billerica, MA.

The SCOMP would be suitable as a gateway or guard.

Multics, Version MR11.0: The Multics system has been assigned an overall evaluation class of **B2**.

> The Honeywell Multics system consists of the Multics operating system running on Honeywell Level 68 and DPS-8M mainframes. These systems include Multics-specific hardware to support the Multics system architecture and protection mechanisms. A large Multics system may be configured with several processors and can support

several hundred users. Multics can be used in a wide variety of environments.

The Multics operating system is a general-purpose time-sharing system with strong security features. Multics has three basic security mechanisms. The hardware-supported protection rings and segmentation provide tightly controlled separate domains of execution. The Access Isolation Mechanism (AIM) software provides mandatory access control. The Access Control Lists (ACLs) provide discretionary access control. [7].

The vendor for the Honeywell Multics system is Honeywell Bull, Incorporated.

Multics systems are currently in use at more than 100 locations worldwide, including NSA, MIT, and the Air Force Data Services Center (AFDSC). As early as 1976, Multics was accredited to operate in Controlled Mode at some DOD sites (TS/collateral and Secret data on a machine shared by TS and Secret users).

Network Operating System (NOS), Version 2.4.1: NOS 2.4.1 has been assigned an overall evaluation class of C2.

The CDC NOS Security Evaluation Package consists of NOS version 2.4.1, TMS4, and the audit reduction tool running in secured mode on the CDC Cyber 170/800 series or Cyber 180/800 series machines. The evaluated system configuration includes only the following subsystems: Network Access Method (NAM); Batch I/O (BIO); Interactive Access Facility (IAF); Magnet (MAG); Remote Batch Facility (RBF); and Tape Management System (TMS). NOS is a large general-purpose time-sharing system capable of supporting several hundreds of users. NOS can be used in a wide variety of applications. The system's protection mechanisms provide a fine-grained discretionary access control over all files on the system [8].

The vendor for NOS 2.4.1 is the Control Data Corporation.

Although NOS provides some mandatory access controls, they are not sufficient to satisfy the TCSEC B1 mandatory access control and labeling requirements. Some mechanisms needed to handle classified information are provided, including identification and authentication mechanisms.

VAX/VMS, Version 4.3: VMS 4.3 has been assigned an overall evaluation class of **C2.**

> VAX/VMS (Virtual Address eXtension/Virtual Memory System) is Digital Equipment Corporation's general-purpose operating system that runs on all VAX systems, including processors ranging from the VAX 11/725 to the VAX 8800. VAX/VMS software provides an environment for concurrent execution of multi-user, time-sharing, batch, and real-time applications.
>
> The VAX architecture provides four processor-access modes that are used to provide read/write protection between user software and system software. Memory and device access is controlled on a per-page basis by processor memory management.
>
> VAX/VMS software provides privilege and protection mechanisms to limit user access to system-controlled structures in physical memory, system-structured files and volumes, and some devices. User accounts are maintained in a User Authorization File (UAF) by a system manager. Each account has a user name and an encrypted password for identification and authentication of the user, and lists the privileges available to the user.
>
> Each account contains a User Identification Code (UIC) which is compared with user-specified file and device access-control lists to provide discretionary access controls. Access-control lists may also be used to identify security events that are to trigger real-time security alarms by access and/or access attempts. Messages are sent to any terminal designated as a security terminal and are also stored in a log file to provide an audit trail of user access activities [9].

The vendor for VAX/VMS is the Digital Equipment Corporation.

UTX/32S, Release 1.0: UTX/32S has been assigned an overall evaluation class of **C2.**

> The UTX/32S system consists of the UTX/32S operating system running on a Gould PowerNode 6000 or 9000 series minicomputer. The UTX/32S operating system is based on Berkeley 4.2 BSD and AT&T System V. UTX/32S preserves the strengths of the UNIX operating system and eliminates many of the security weaknesses while maintaining almost complete command and system library compatibility.

UTX/32S implements an additional integrity mechanism, called the Restricted Environment, to provide isolation between privileged (trusted) and unprivileged domains. Unprivileged users operate in the restricted environment. This restricted environment, which is a subtree of the file system, is a virtual UNIX system containing all common untrusted programs and files. TCB files and privileged programs are kept outside this environment and thus are protected from modification by untrusted users. Trusted servers perform the sensitive services, including system mail, printing, and device allocation. Only system administrators may access the trusted domain.

To further enhance security, UTX/32S eliminates some of the weaknesses inherent in UNIX, including the "setuid" feature on files. Discretionary access control is provided by the standard UNIX protection-bit mechanism. In addition, UTX/32S provides a stronger I/O device control mechanism [10].

The vendor for UTX/32S is Gould, Inc., Computer Systems Division.

A Series MCP/AS with InfoGuard Security Enhancements: A Series has been assigned an overall evaluation class of **C2**.

A Series is the current family of fully compatible computers produced by UNISYS Corporation. Members of the product line range in size from several-user minicomputers to mainframes supporting hundreds of users. The product line currently includes 21 models of processors that offer more than a 270-fold performance range. The A Series system architecture is based on the high-order language, ALGOL. The A Series system supports reentrant/recursive multiprocessing, multiprogramming, and virtual memory through its tagged memory and stack architecture.

Software for A Series includes the Master Control Program/Advanced System (MCP/AS), Infoguard security improvements, a broad range of high-order language compilers, COMS (data communication interface and transaction processing controller), CANDE (user/programmer time-sharing interface), DMSII (data management), and a full complement of utilities. The A Series Trusted Computing Base (TCB) is composed of MCP/AS, InfoGuard security improvements, the compilers, COMS, CANDE, and many system utilities. TCB software provides privilege and protection mechanisms to mediate and monitor access to system and user resources.

All processors in the A Series product line provide a single state for execution. Therefore, the A Series system software is responsible for providing a self-protecting domain for the A Series Trusted Computing Base (TCB). Although in many systems, isolation of the TCB from user processes is provided by running the TCB in a completely separate (and privileged) hardware protection state, this is not true of A Series. Instead, a combination of capability-like hardware mechanisms and TCB software (including the compilers) is used to provide the necessary isolation. Because programs compiled by unprivileged users have no direct access to the machine instruction set or to the hardware enforcement mechanisms, the A series TCB is able to isolate itself and other user processes from any attempted security violations. These capability-like hardware mechanisms are the tag architecture, the base and limit of stack registers, and the display registers [11].

The vendor for A Series is UNISYS Corporation.

Add-on Packages

Several vendors have released add-on software security packages for IBM systems running the MVS operating system. Information relating to these products follows.

Access Control Facility 2 (ACF2), Release 3.1.3: ACF2 has been assigned an overall evaluation class of C2.

The ACF2 security subsystem is designed to provide security for data stored on computer systems using the IBM MVS or VSI operating system. ACF2 provides protection by default for data sets resident on Direct Access Storage Devices (DASDs), IBM 3850 Mass Storage Systems (MSS) and tape volumes. Protection levels of READ, WRITE, ALLOCATE (allocation, rename, scratch, and catalog functions), and EXECUTE-only are supported. Interfaces between ACF2 and many popular commercial software products are provided by SKK. These software products include Information Management System (IMS) and Customer Information Control System (CICS) by IBM [12].

The vendor for ACF2 is SKK, Inc.

TOP SECRET, Version 3.0, Level 163, with Feature Option #43: TOP SECRET has been assigned an overall evaluation class of C2.

> TOP SECRET is an add-on security package developed by CGA Software Products Group, Inc., for IBM's Multiple Virtual Storage (MVS) operating system. TOP SECRET provides default protection of system facilities, data sets resident on DASD devices, and DASD and tape volumes. TOP SECRET also provides the capability for decentralized access control through several layers of security administration, extensive audit features (both on-line and batch), and the capability to gradually implement the security provided by the TOP SECRET package.
>
> Interfaces between TOP SECRET and many commercial software products are provided by CGA. These include: Information Management System (IMS), Customer Information Control System (CICS), ROSCOE, COMPLETE, TSO, IDMS, PANVALET, and others [13].

The vendor for TOP SECRET is CGA Software Products Group, Inc.

Resource Access Control Facility (RACF), Version 1, Release 5: RACF, Version 1, Release 5 has been assigned an overall evaluation class of C1.

> RACF is an IBM MVS facility that provides controlled access to system resources. RACF with MVS/370 was the evaluated configuration; however, RACF is also supported under MVS/XA. RACF is designed to limit access to resources by identifying authorized users and protected resources, then controlling users' access to those resources. RACF also provides the security administrator with the option of default protection on permanent Direct Access Storage Device (DASD) data sets. RACF provides protection for data sets resident on DASD, IBM Mass Storage Systems (MSS), and tape volumes. Access levels of ALTER, CONTROL, UPDATE, READ, and NONE are supported for DASD data sets. Interfaces between RACF and other IBM products, including Information Management System (IMS) and Customer Information Control System (CICS), are supported by IBM [14].

The vendor for RACF is IBM Corporation.

These add-on packages previously described supplement the security capabilities of MVS with specific capabilities for controlling access to system resources. Although each package started out with distinct advantages and

disadvantages, now they all provide roughly equivalent services. All of these packages supplement access control to the machine itself and provide improved audit trails of system activity.

These systems were evaluated in 1984 and 1985 on the MVS/SP operating system, although they will run on a variety of IBM 370-type systems. This type of add-on package is no longer evaluated as a separate entity for a class rating by the NCSC because it is felt that they are too easily subverted by someone with a knowledge of security flaws in the underlying operating system. An add-on package must now be evaluated in conjuction with its underlying operating system for a class rating.

PRODUCTS BEING EVALUATED

Digital Equipment Corporation Security Enhancement Service (SES): SES is an add-on security package for VAX/VMS 4.4 which runs on all VAX systems, although VAXclusters and VAXstations may not be supported. VAX/VMS with SES is currently in developmental evaluation with the NCSC for a B1 rating.

Gemini Computers, Inc., GEMSOS Operating System: GEMSOS, a secure distributed operating system, is presently under development. GEMSOS is expected to accommodate from 1 to 8 processors. Gemini has completed work on the security kernel of GEMSOS, and is now working on the system supervisory layer of GEMSOS, which together with the kernel provides a complete distributed operating system. Gemini has plans to develop a secure UNIX-compatible operating system to run on top of the supervisory layer of GEMSOS. LAN interface standards and protocols currently supported include RS232 and HDLC, and Gemini has plans to implement TCP/IP. GEMSOS is currently under developmental evaluation at the NCSC for a B3 rating; completion of the evaluation is expected in 1988-89.

UNRESOLVED ISSUES

The area of multi-user, general-purpose hosts is the subject of much research. Security inevitably affects performance because it requires the computer to do more work. For true multilevel security, each reference to an object must be checked to ensure that the subject is authorized to use that object in the way specified by the reference. This fine-grained control of resources is necessary in a secure computer system to provide the same capabilities found in non-computerized secure environments.

Work at the NCSC is progressing on the evaluation of B2 or higher general-purpose operating systems for various minicomputers and superminicomputers. Because of proprietary concerns, very little can be said of work under developmental evaluation at the NCSC. B2 or higher operating systems for minis and superminis should be commercially available and on the EPL within the next 3 to 5 years.

Although B2 or higher systems may not provide full multilevel secure capabilities, they would allow secure sharing of data between two or possibly three consecutive levels, such as Secret and TS or TS and TS/ESI, possibly Secret, TS, and TS/ESI. Even this "controlled mode" of operation possible with B2 or higher systems could be useful in reducing the cost of secure computing.

SECTION 3

DATABASE MANAGEMENT SYSTEMS

DEFINITION

A Database Management System (DBMS) is an integrated set of software tools allowing concurrent shared access to a database and providing sophisticated manipulation of data items within that database. DBMS products are not limited to run on computers of any specific size.

ISSUES

Secure database systems are still in the research stage. Numerous problems have yet to be solved, including inference (when non-releasable information can be derived from authorized information) and aggregation (when several data items taken together have a higher classification than any one of them alone).

STANDARDS AND GUIDELINES

The NCSC is supporting an effort to interpret the TCSEC specifically to evaluate DBMSs [15]; this will probably be completed within the next two years. Draft guidelines for B1 and below DBMS products may be available soon, with interpretations for the higher classes to follow. DBMS product evaluations, inference, aggregation, and many other issues will be discussed before the Trusted DBMS Guidelines can be published.

CURRENTLY AVAILABLE PRODUCTS

There are currently no commercially available secure DBMS products evaluated by the NCSC. While most DBMS products provide some security mechanisms, they are not designed to enforce DOD security policy or to take advantage of an underlying computer system's trusted computing base. Therefore, most commercially available DBMSs lack the assurance that a DAA would require.

RESEARCH AND DEVELOPMENT

Three approaches to building security controls into DBMS products were examined in the 1982 Air Force Summer Study [16]: integrity lock, Schaefer-Hinke, and kernelized DBMS.

In the kernelized DBMS approach, new DBMS products are developed according to the TCSEC criteria as extrapolated and interpreted for DBMSs. Using this approach, the security critical functions of the DBMS are isolated, the resulting kernel of functions is demonstrated to be trusted, and therefore, the DBMS as a whole can be "trusted." The DBMS is developed with respect to a specific operating system, and the DBMS must interact with the operating system in a trustworthy way. Because the kernelized DBMS approach requires the design and development of an entirely new class of DBMS products, it is viewed as a long-term approach not likely to meet operational requirements for some time to come (5-7 years). The Mermaid system, currently under development by System Development Corporation, is using this approach.

The Schaefer-Hinke approach was conceived as a short-term solution where the database itself is reorganized to take advantage of the tools provided by a secure operating system for managing files and devices. In this way, currently available software, including a DBMS and its underlying operating system, would be modified and then used to provide some measure of protection to a current database. The protection would grow with the emergence of more secure operating systems. This approach, named for the researchers who first devised it, has evolved into a long-term approach where a DBMS is designed to use, complement, and expand upon the security policy enforced by the secure operating system. This is contrasted with the kernelized approach, in which the operating system and the DBMS could be written to enforce different security policies. There are problems with efficiently maintaining database integrity and with implementing special-purpose views. At present, no systems implement the Schaefer-Hinke approach.

Integrity lock is a short-term approach using a commercial DBMS retrofitted to provide security. A trusted filter is installed between the DBMS software that has access to records and the DBMS software that interacts with the user [17]. The filter computes an unforgeable cryptographic checksum based on the data and its classification. This effectively seals the data with its security level. Any unauthorized modifications to the data or its security tag can be detected when the data is retrieved. The operating system needs to be able to ensure to a reasonable degree that access to the DBMS data files can occur only by going through the trusted filter. This approach allows a modified version of a currently available DBMS to be used on a commercial operating system, and probably is the best hope of practical results in the near term.

SECTION 4

WORKSTATIONS

DEFINITION

Workstations usually support only one user at a time, and are frequently special-purpose machines, meant to satisfy specific needs of the user. Technically, personal computers fall into this category, although they are usually more general in purpose than workstations. Workstations are built on one or more microprocessors, with the extra processors dedicated to specific tasks such as I/O or graphics.

ISSUES

Workstations present different aspects of computer security because the user now has control of the system. The operating system is usually programmable by the user, who may also have access to the communications system of the network it is connected to. The increasing power available to these workstation users to communicate with other workstations and with mainframe hosts increases security risks.

Control of the kinds of disk storage in a workstation can be used to provide a certain amount of security control. Some workstations do not provide any means of protecting data among various individual users operating on it one at a time because their operating systems were written for single users. Security issues differ between stand-alone workstations and workstations connected to a network or a host. When different users use a stand-alone workstation, the storage of data on fixed disks by the individuals must be mediated and the data residue purged. Without proper protection or accountability, other user's files may be read, copied, altered, or deleted.

The issues for communicating workstations include those for stand-alone, with additional issues raised because the user can communicate with other workstations and hosts. Software of unknown integrity can be loaded from remote systems and executed at the workstations, introducing the potential for Trojan Horses and trapdoors. The user at a workstation also has access to information from other systems. The workstation provides an automated mechanism for performing exhaustive, repetitive actions that are an ideal mechanism for attacking remote systems without sufficient security protection.

STANDARDS AND GUIDELINES

The TCSEC provides security guidelines for systems configured in the traditional configuration of a mainframe with terminal attachments. It provides a very good basis for developing criteria for secure workstations because most workstations perform a subset of traditional operating system functions. The evaluation of the security impact of workstations on a system may also be determined by the TNI.

DIA has been using Compartmented-Mode Workstations (CMW) to create a compartmented-mode network (DNSIX and SACINTNET) over which the workstations has access to system high or dedicated (multi-user) hosts. This is planned to allow DIA-supported installations to exploit the power of their current computing and human resources more fully without waiting for the development of compartmented-mode hosts.

CURRENTLY AVAILABLE SYSTEMS

There are currently no evaluated, commercially available secure workstations.

DEVELOPMENT INITIATIVES

Several vendors are developing workstations with security features. A brief summary of this work follows.

- IBM Federal Systems has announced that its Xenix-based secure operating system for IBM PC/ATs, currently in developmental evaluation with the NCSC at a B2 level, will be available soon. IBM sales people have indicated that this product advanced to the formal evaluation process at the NCSC in 1987, and they expect it to be placed on the EPL as a B2 system sometime in 1988.

- SUN Microsystems is working on a workstation featuring UNIX. SUN has not yet entered developmental evaluation with the NCSC, but has targeted its effort for a B1 rating.

- Gemini Computers, Inc., is developing a secure distributed operating system (GEMSOS) on the iAPX 286, the chip also used in the IBM PC/AT.

- DIA has been sponsoring work in CMWs. These workstations are intended for use by intelligence analysts who must routinely work with data classified into different compartments, gathering, analyzing, synthesizing, and disseminating information without causing data to be wrongly classified at any step of the process. In its most highly automated form, this process currently requires two or more separate terminals and a fair amount of manual effort. CMWs are being developed to assist analysts in these tasks.

- Requirements for a CMW have been approved by DIA and a modified version of these requirements has been adopted as a DIA standard for compartmented-mode systems in general. MITRE has built a working prototype of a CMW, and acquisition efforts are beginning for DIA projects.

- IBM has based its CMW effort on its Secure Xenix operating system already in developmental evaluation with the NCSC, and has announced that its Compartmented-Mode Workstation software for IBM PC/ATs will be available soon. IBM plans to request DIA certification of its CMW.

- SUN Microsystems is planning to build its CMW effort on its secure UNIX operating system currently under development. Because SUN's workstations are already so successful, their CMW effort may provide a very satisfactory tool for intelligence analysts.

- Masscomp has bid on an NSA contract for multilevel secure workstations, but they lost the bid and little is known about what security measures they have actually implemented in their UNIX-based workstation.

SECTION 5

NETWORKS

DEFINITION

A Network is an interconnected collection of autonomous computers that supports communication between different independent host processors, workstations, I/O devices, and other networks. This section covers traditional long-haul networks, Local Area Networks (LANs), and networking devices such as gateways and bridges.

LANs are distinguished from long-haul networks primarily by the limited physical area they cover and the consequent increase in data rates possible because of the short distances involved. LANs can connect users whose terminals or workstations are up to 20 km apart, although more typical distances are less than 0.5 km (within a single building or complex of buildings). Some draw the distinction between LANs and long-haul networks less strictly by using the concept of communities of interest to describe the area served by a LAN.

A gateway is a device which allows data to be be transferred from one network to another. In general, the two networks support different protocols and the gateway performs the required protocol conversion. The networks on either side of a gateway may be long-haul or local area. Gateways are sometimes included as an optional LAN interface by a vendor, as an integral part of the LAN product.

In 1978 the International Standards Organization (ISO) recommended a seven-layer model for network architecture; this model is known as the ISO model for Open Systems Interconnection. The layers are: 1 = physical link layer; 2 = data link layer; 3 = network control layer; 4 = transport layer; 5 = session control; 6 = presentation control; 7 = application/user layer.

Bridges allow the transfer of data between networks which have dissimilar protocols only at the lowest levels of the ISO model. Since security is usually addressed in the higher levels of network protocol (layers 4 through 7, with 5 being typical), bridges usually have no unique or specific security functions.

ISSUES

LANs are simpler and newer than long-haul networks, and therefore have been a focus of much attention in the security field. Adding security to a LAN is perceived to present a more tractable problem than traditional networks. Both need to solve the same security problem: how to provide secure communications services among subscriber systems with potentially different security levels.

The security problems in a network include those of a host computer, but networks also have additional problems, including data integrity, denial of service, eavesdropping, and maintaining the separation of classification/category levels of the data being passed over the network.

STANDARDS AND GUIDELINES

The NCSC has developed the *Trusted Network Interpretation* (TNI) [4] of the TCSEC as a guideline for evaluating security in networks.

The first section of the TNI is an interpretation of the TCSEC for networks. This section develops a theory and structure of secure networks based on the TCSEC concepts of computer security. There are two key ideas presented in this section: the first is the definition of the Network Trusted Computing Base (NTCB); the second is the notion that network components can be evaluated separately against specific policy categories. The NTCB is a Trusted Computing Base distributed across a number of different network components, which when interconnected, can be shown to support the network's security policy. A network component may be a host, a workstation, a guard device, or a data communication system. Each of these components may be evaluated separately, and each network component may support some, all, or none of the functions of the NTCB.

The second section of the TNI addresses security services peculiar to networks which are not covered by the interpretation of the TCSEC. These security services are Authentication (Peer Entity and Data Origin), Data Confidentiality, Data Integrity, Non-Repudiation, Denial of Service, and Support Primitives (Encryption, Testing, Protocols). These security services are based on the ISO security protocols and do not have to be part of the NTCB.

Appendix A of the TNI develops an approach to the evaluation of individual network components. Appendix B provides a rationale for the NTCB partitioning of a network for evaluation with these interpretations.

Appendix C presents a third key idea of the TNI, that of interconnection rules for accredited but not necessarily evaluated or certified component systems. These rules are first examined from a local point of view, at the level of a component and its neighbors. From a global view, interconnection rules center on a consideration of the cascading problem present in any network whose components have different accreditation ranges. Appendix C formalizes a heuristic for determining whether a specific network meets the criteria discussed from both a local and a global view.

LANs and other devices which can be categorized as network components will probably be evaluated against the two main sections of the TNI using the approach outlined in Appendix A.

All of the networks in operation today consist of interconnected, accredited, but probably unevaluated systems, which is what makes Appendix C of the TNI such an interesting proposition; Appendix C is likely to be the part of the TNI applicable to the greatest number of situations.

CURRENTLY AVAILABLE SYSTEMS

Significant security features have already been implemented in networks currently used. DOD's secure long-haul networks are built on contract specifically for DOD. DIA has invested in and continues to work on its own secure long-haul network, DODIIS. DODIIS, together with the SACDIN, WIN, and other non-intelligence networks, is being merged into the Defense Data Network (DDN). It is under this umbrella program that most of the development of long-haul secure networks is being done for DOD.

RESEARCH AND DEVELOPMENT

As mentioned above, research and development of secure and multilevel secure (MLS) long-haul networks is progressing under the DDN. Specifically, BLACKER and Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE), both of which would be categorized as network components by the TNI, are featuring the new DOD encryption standard and are being developed and evaluated by NSA; BLACKER should be available within the next two years.

Some see the emerging CCEPs (Commercial COMSEC-Endorsed Products) as the answer to all network security problems, and indeed, encryption is very important over a long-haul network. If CCEP makes approved encryption techniques available and practical for more applications, for example, in the form

of fast encryption chips, then many advances may be expected in the near future. Several networks and network products in development are planned to use encryption to guarantee separation of levels and to provide user authentication and unitary logon.

Regardless of the advances in technique which may result from CCEP, the framework suggested by the NCSC's TCSEC raises questions that cannot be answered by any one technique. Encryption cannot by itself provide accountability, although it may make that task easier. Problems such as Trojan Horses, covert channels, and aggregation will remain despite encryption.

Development of MLS LANs is underway at a number of different commercial companies, most of whom are planning to place their products in evaluation at the NCSC. A few are already in developmental evaluation.

The Boeing MLS LAN effort appears to be further along than any of the others. Boeing is currently in developmental evaluation with the NCSC for an A1 rating.

A recent advertisement describes several attributes of the Boeing MLS LAN:

"The Boeing MLS LAN separates computers, users, and data flowing between computers, providing controls to preserve different data sensitivities simultaneously among computers connected to the same network. Yet it also allows data to flow between differing levels if appropriate, such as from confidential to secret, and not the reverse. Access control is provided for both single-level and multilevel users and devices."

"The Boeing design uses fiber optics and wavelength division multiplexing to permit simultaneous transmission of multiplexed digital and voice (100 MBPS), video, and high-speed digital stream data (300 MBPS) [18]."

The Boeing LAN will, as noted, provide a video interface; also, it provides ordinary RS232 terminal and host interfaces, but not host-resident interface software (estimated by Boeing to be approximately 5000 lines of code per interface). The Boeing LAN supports X.25, Ethernet, and TCP/IP. Boeing currently has DR11 interfaces for VAXes, SUN workstations, and PCs, but does not yet have an IBM Channel Interface.

The Verdix LAN is another effort in the final stages of development. Verdix was the first company to enter developmental evaluation with the NCSC

with an MLS LAN product (August 1985). The system was designed as an A1 system, but Verdix has since dropped the target evaluation class to B2. Verdix LANs are now in beta testing at several sites.

There are two major components associated with the Verdix Secure LAN: the Network Security Device and the Network Security Center. The Network Security Device provides access mediation at each node, and the Network Security Center provides for network-wide security administration and control.

TRW, Litton-Amecon, and others have working prototypes of MLS LANs, and several other vendors, including IBM, appear to be working on prototypes of their own.

By 1990, MLS LANs should be listed on the NCSC's Evaluated Products List and available off the shelf, but their installation, certification, and accreditation in particular environments will still be fairly complex and, in some cases, very costly.

SECTION 6

GUARDS AND GATEWAYS

DEFINITION

A guard is a trusted computer system interposed between two other systems computers, networks, or terminals operating at different security levels. The guard is trusted to mediate all information transfer between the two security levels to ensure that no sensitive information from the higher level can leak to the lower level and to protect against destruction of data on the high level. A guard is a small special-purpose system that can be isolated from the systems it connects.

Guards may be fully automated, requiring little or no human intervention, or they may be partially automated, using only the display and storage capabilities of the machine, and relying on human review and response for all decisions. Guard functions can be built into a workstation, a multi-user host, or a network gateway, but it is most likely that a guard function will be built into a unique device which is constructed expressly to act as a guard in a particular situation.

Gateways are also small special-purpose systems that allow the exchange of information between different networks. The networks on either side of a gateway may be long-haul or local area, with either similar or dissimilar protocols. Gateways are sometimes included as an optional LAN interface by a vendor, as an integral part of the LAN product. Gateways can be viewed as a two-way guard between networks. Although gateways have additional functions, including protocol conversion and routing, their security functions are similiar to those of guards: they mediate access between systems operating with different security levels.

ISSUES

Currently, two common practices to transfer data across security boundaries of systems are manual review and reentering of data and some form of media transfer. Guards are an attempt to provide interoperability between systems operating in different modes by automatically transferring data across security boundaries. A defense must be provided against unauthorized data disclosure, data integrity violations, and denial of service. The guard must also prevent penetration of one system by another.

Several new issues arise when guards are used to replace current transfer practices [19]. Implementation can be centralized or distributed. Centralized guards provide centralized control and a single audit trail, but distributed guards are more survivable. Guards also create new information channels, and the increased data flow increases the risk.

In the paper, *Security Guards: Issues and Approaches* [19], previous efforts to produce guards for the DOD are examined, as are several characteristics that contributed to their failures such as:

1. The guards introduced additional workstations, hosts, or specialized hardware as well as complex software.

2. Some guards required substantial hardware or software changes in the systems being supported.

3. The guards all sought high degrees of technical security, and were expensive and time-consuming to develop.

4. Guard operation and administration often were cumbersome.

The paper suggests that these characteristics are symptoms of two underlying problems: a lack of user commitment and lack of sufficient policy guidance.

STANDARDS AND GUIDELINES

The NCSC does not have guidance specifically for the evaluation of guard devices. The Trusted Network Interpretations would probably classify most guard devices as network components, and as such, responsible for enforcing some aspect of overall network security within a specific network environment. However, a strict reading of the TNI's Appendix C: *Interconnection Rules for Accredited Systems* rules out the possibility of a fully automated guard between some systems because of the cascading problem explored in the Network section.

CURRENTLY AVAILABLE SYSTEMS

Guards are application-specific interim solutions to the problem of unavailability of true MLS systems. Operational guard devices are usually custom-made or at best customized, and are usually not COTS (Commercial Off The Shelf) equipment. The best hope for cutting costs in implementing guard functions is to build a guard application on a COTS gateway product with a Trusted Computing Base (TCB), possibly combining this with an MLS

workstation for manual downgrading, or control of the gateway. The most significant savings here is gained through the reuse of the trusted code in the gateway and workstation products.

Because there is so little guidance on the matter, and because guard devices almost inevitably affect more than one organization's mission effectiveness and power base, they are usually built in a politically charged atmosphere. As a result, very few guard systems ever built have been accredited and put into operation. Two systems that are currently operational are: a semi-automated guard workstation tool developed for the U.S. Army in Europe; and NASA's fully automated Restricted Access Processor (RAP). Both operational guards and guards which were built but never fielded are of interest for this assessment not primarily because of their technical sophistication, but for lessons learned during their development.

As mentioned in Section 2 of this document, the Honeywell SCOMP, evaluated at A1 by the NCSC, would be suitable for a guard.

Overviews of previous attempts to build guards follow.

ACCAT GUARD: The Advanced Command and Control Architectural Testbed (ACCAT) Guard was built to allow controlled two-way information interchange between a Top Secret/Sensitive Compartmented-Information network and a Secret network. The ACCAT Guard required human review.

FORSCOM: The U.S. Army Forces Command (FORSCOM) Security Monitor (FSM) was developed as an experimental system to test the operational impact of a guard in the FORSCOM environment. The FSM was intended to allow terminals operating at the Secret level to be connected to a Top Secret network. The FSM used three mechanisms to prevent illegal information flow: automatic screening of fixed-format output; human screening; and filtering of user commands and file names.

LSI GUARD: The LSI Guard, a microprocessor guard system contained in a single terminal, is a single-user system to connect two systems at different levels. The user may be connected to either the high or the low side, or can act as a review officer for data moving between the two sides.

KAIS: The Korean Air Intelligence System (KAIS) Security Interface is intended to allow sharing of data between systems operating at two different security levels.

MFM: The Message Flow Modulator (MFM) is intended to be a generic guard suitable for use in different applications. It is designed to be completely verifiable, and to be tailored by the user. The modulator controls the flow of messages from a source to a destination. Two modes are available, manual and automatic.

RAP: The Restricted Access Processor (RAP) allows NASA's Network Control Center to support classified and unclassified users and data. RAP processes input and output messages by examining the source and destination fields and the function of the message. Only messages with valid headers and subfields are forwarded; all others cause an operator alert.

RESEARCH AND DEVELOPMENT

There are three projects currently under development which might provide a generic base on which to build reliable guard functions for specific systems. These are Sytek's Trusted Domain Machine (TDM), Ford Aerospace's Multinet Gateway, and Gemini's distributed operating system GEMSOS. All are being developed according to TCSEC principles and plan to obtain NCSC endorsement.

Sytek's TDM is designed specifically to provide a TCB for secure application ;, with guard functions as its primary target application. The TDM is a Motorola 68000-based machine which uses local buses and specially modified memory boards to provide domain separation between data on both sides of the interface. The "core" software is trusted to transfer data between domains properly. Sytek has completed this "core" software for its project sponsor. Development of an application for this device would require the purchase of a TDM, purchase or lease of a development environment, purchase or lease of the TDM software, and the cost of developing the application itself. This is still less expensive, however, than completely developing a one-of-a-kind system.

Ford's Multinet Gateway project originated as a Rome Air Development Center (RADC) technology-transfer project. Its basic function is to assist the survivability of DOD networks below the transport layer by providing internetting capabilities between heterogeneous backbone networks, as well as to guarantee

the integrity of the data classification labels passed through it at the network layer. Multinet Gateway was built using TCSEC A1 principles as a guide. The Trusted Computing Base (TCB) provided by the Multinet Gateway can be used as the base for specific guard functions. Again, this could save some of the expense involved in building one-of-a-kind guard systems. Multinet Gateway is currently under evaluation and certification by NCSC.

Gemini's distributed operating system for the Intel 286/386 family, Gemini Secure Operating System (GEMSOS), could also be used as a base for an MLS or controlled-mode guard function. Gemini is building GEMSOS specifically for use in DOD communications systems, and is planning to allow up to 8 processors to be run concurrently within a single device. Gemini has completed work on the secure kernel of GEMSOS, and is now working on the system supervisory layer of GEMSOS, which, together with the kernel, would provide a complete distributed operating system. LAN interface standards and protocols currently supported include RS-232 and HDLC, and Gemini has plans to implement TCP/IP support. GEMSOS is currently under developmental evaluation at the NCSC for a B3 rating; completion of the evaluation is expected in 1988-89.

SECTION 7

MISCELLANEOUS COMPUTER SECURITY PRODUCTS

INTRODUCTION

In addition to products discussed in previous sections, there are several other hardware and software items designed to improve computer security. Some of these products appear on the NCSC's EPL, and some do not. In the February 21, 1986, issue of *Commerce Business Daily,* there was a Request for Information (RFI) on these types of products [20]. The following paragraphs summarize the responses to the RFI.

PRODUCTS CURRENTLY ON THE EPL

Each subsequent paragraph contains the name of the product, the NCSC "Product Description" as it appears on the EPL (in indented format), and the name of the vendor. Vendor addresses are listed in Appendix A.

> **Access Control Encryption (ACE) System:** ACE is an integrated hardware/software package which provides user identification and authentication (I&A), trusted path to the host, and audit on I&A mechanisms for a host computer system. It is composed of two distinct components. The first, the Access Control Module (ACM), is a stand-alone device that is installed such that all communication channels to the host system must pass through its protection mechanisms. ACE's stand-alone design provides basic security mechanisms to computer systems that implement no security mechanisms of their own. The second component is the SecurID card which every user must possess in order to identify himself to the ACM [21].

The vendor for the ACE System is Security Dynamics, Inc.

> **CPP-300 Trusted Path Port Protector:** The Codercard Trusted Path Port Protector is a user authentication mechanism for use with computer systems that either lack a user authentication capability or require additional authentication assurance. It is designed to operate in pairs, and to protect a single asynchronous communication path

between computers or equivalent devices such as terminals. In order for the authentication to be successful, the Codercard Reader at each end of the communication line exchanges a series of random numbers with the Codercard at the other end. In this way, a two-way challenge-and-response authentication is accomplished. Only after exchanges have been completed successfully in both directions is access to the communication line granted [22].

The vendor for the CPP-300 is Codercard Inc.

Gordian Systems Access Key, Release Version A.00: The Gordian Systems Access Key product is a user authentication mechanism for use with computer systems that either lack a user authentication capability or require additional authentication assurance. The Access Key product is a challenge-and-response device. After a user has identified himself to the host system, the Access Key system "challenges" the user by flashing a stimulus on the terminal screen and waits for the user to enter the proper password response. The user attains the correct password by holding the Access Key device to the terminal screen and allowing it to read and decrypt the visual challenge. The Access Key device returns the appropriate six-character password on its LCD display. The Access Key system consists of the domino-sized Access Key, software that is integrated with the host system, and a "Key Cutter" device that initializes each Key with a unique encryption profile [23].

The Gordian Systems Access Key is manufactured by Gordian Systems Incorporated.

SafeWord UNIX-Safe: SafeWord UNIX-Safe (Safeword) is a software package which, when running under the XENIX operating system, provides an identification and authentication (I&A) mechanism for users, and auditing of this mechanism (audit). The security mechanisms can be used either independently or as supplements to those already provided by the underlying operating system. The I&A mechanism requires that each user first provide a user identifier (ID). This ID is used by SafeWord to generate a challenge for the user. The user must first enter his personal identification number and then the challenge into a small, hand-held, pseudo-random-number-generating device. In return, the hand-held device generates a response with which the user may then complete the login sequence to the host system [24].

The vendor for SafeWord UNIX-Safe is Enigma Logic, Inc.

Sentinel Security System: The Computer Security Corporation's Sentinel Security System can be an effective addition of security to an IBM PC, PC/XT, PC/AT or true-compatible microcomputer. Sentinel is an integrated hardware/software package capable of providing access control to programs and files (discretionary access control), user logon procedures (identification and authentication), and auditing of user actions (audit). In addition to these security features, Sentinel also prevents unauthorized attempts to format the non-removable hard disk, and has the ability to encrypt programs and files (protected objects) [25].

The vendor for the Sentinel Security System is Computer Security Corporation.

SGT SECURITY: SGT SECURITY is a microcomputer software package which operates on IBM PC, PC/XT, PC/AT, or BIOS-compatible microcomputers under MS-DOS or PC-DOS. The product provides procedures to clear the internal magnetic media (floppy and Winchester disks) and random-access memory. The user interface is command driven from a single screen which displays menu selections to perform the functions. The company provides both a user manual and a more detailed security officer manual with the product [26].

The vendor for SGT SECURITY is Pike Creek Computer Company, Inc.

Sytek PFX A2000/A2100 (PFX Passport): The Sytek PFX (model numbers A2000 or A2100), in conjunction with the PFX Passport, is intended to serve as a user authentication mechanism for use with a wide range of host architectures. The Sytek PFX A2000, which runs on a PC/AT (or compatible), and the Sytek PFX A2100, which runs on PC, PC/XT, and PC/AT computers, were both evaluated by the National Computer Security Center. Each of these systems consists of a microcomputer (IBM PC/AT or compatible), associated software, and a hand-held Passport device. For use, a system user enters his personal identification number into the Passport. He then enters his login identification to the host system which prompts him with a 7-digit challenge and waits for a response. This challenge is entered into the Passport device which combines it with seed information to produce a 7-digit response. The user then enters this response to the host machine, allowing access only if the challenge response is equivalent to the one generated by the PFX A2000 system [27].

The vendor for Sytek PFX A2000/A2100 is Sytek, Inc.

Triad Plus: Triad Plus is an add-on security product which, when implemented on any IBM PC/XT or PC/AT configured as tested, provides user Identification and Authentication (I&A), Discretionary Access Control (DAC) on objects, DAC on system resources (RAC), Object Reuse, and Audit mechanisms. Once a user has logged onto the workstation, these mechanisms are essentially transparent. Unless the user attempts to exceed his defined privileges, the only noticeable difference is a slight degradation in workstation performance. Triadtrator may use them. In addition, Triad Plus comprises an expansion board, personal identification tokens, and some supporting software utilities. The expansion board itself provides all of the security mechanisms. These mechanisms are used in conjunction with a personal identification token used to provide a physical element in the authentication process. The software utilities are provided for the convenience of users. However, some utilities are privileged – only a workstation administrator may use them. In addition, Triad Plus uses an intricate memory management scheme, referred to as the Controlled Access Mechanism (CAM), to protect the resources on its expansion board. The CAM disallows random access to the information on the board by allowing access only through specific controlled entry points within the workstation's address space [28].

The vendor for Triad Plus is Micronyx, Inc.

Watchdog PC Data Security, Version 4.1: Watchdog is an IBM PC/XT or compatible software package which provides user access control to programs and files (discretionary access control), user logon procedures (identification and authentication), user auditing (audit), and users' data remanence protection (object reuse). In addition to these highly desirable security features, Watchdog also provides some protection against unauthorized attempts to format or read the data stored on the fixed disk. Watchdog provides additional data protection by encrypting stored information [29].

The vendor for Watchdog, Version 4.1, is the Fischer-Innis Systems Corporation.

PRODUCTS NOT ON THE EPL

The following products are not contained on the NCSC's EPL. In each case the product is identified by name, with the name being followed by a brief description of the product; this description is consistent with information provided by the vendor. In addition, the name of the vendor is provided (vendor addresses are listed in Appendix A).

CypherMaster: CypherMaster is a data encryption software package which involves an implementation of the National Bureau of Standards Data Encryption Standard (NBS/DES). Systems supported by CypherMaster include the IBM PC under MS-DOS, DEC 11 family under RT-11 or RTX-11, and the DEC VAX family under VAX/VMS. The vendor for CypherMaster is CypherMaster, Inc.

Data Physician: Data Physician is a software virus detection and removal package which runs on the IBM PC and compatibles. The software is able to detect a virus by comparing a copy of an original computer program with its current status. By using a mathematical sampling technique, segments of code which infect the program are detected and eliminated. The vendor for Data Physician is Digital Dispatch, Incorporated.

Delta Data 8400T TEMPEST Personal Computer: The 8400T is a total IBM PC-compatible which meets NACSIM 5100A TEMPEST Requirements. Features of the 8400T include detachable dual 360K floppy disk drives and key-lock power switches. The vendor for the 8400T is Delta Data Systems Corporation.

DPS-800/12: DPS-800/12 allows dial-up access to a computer system. Only users with valid passwords have access to the DPS-800 and the computer system it is protecting. The DPS-800 contains its intelligence in the controller module, thus allowing data security to be totally under the control of the data security officer. The product provides an extensive audit trail which notes each activity of the system. A plug-in code key, known as the UV-1, prevents unauthorized users with valid passwords from gaining access to the system, since a unique serial ID and access code are needed before a login is allowed. The vendor for this product is Spectrum Mfg., Inc.

EyeDentification System 7.5: EyeDentification System 7.5 employs the retinal blood vessel pattern of the eye to establish positive identification. There are three modes of operation: enrollment, recognition, and PIN (Personal Identification Number) verification. Features include time zone control, error count with audible alarm, tamper alarm, and non-volatile database storage with a memory capacity to 1200 enrollees. With 1200 eye signatures in memory, and in

the PIN verification mode, memory search and eye signature verification is said to take approximately 1.5 seconds. The vendor for EyeDentification System 7.5 is EyeDentify, Inc.

IDX-10LN: IDX-10LN is an optical fingerprint scanning device. A two-step process is involved: enrollment and subsequent comparison for identification. It is possible for the system associated with this product to store fingerprint templates on 5000 users, with a response time of 7 seconds or less. The IDX-10LN is available in a basic configuration, as a stand-alone terminal, or as a component of a networked system. Up to 62 IDX-10LN terminals can be interconnected to a host processor using a LAN. The vendor for the IDX-10LN is Identix, Incorporated.

Ridge Reader: Ridge Reader uses the ridge characteristics (minutia content) of a live fingerprint to allow or deny an individual access to a secure environment. The product can increase protection of physical areas, data files, and communication lines between computer systems. Enrollment time varies from 3 to 5 minutes, with the average access time being 5 seconds. The vendor for Ridge Reader is Fingermatrix, Inc.

THE KEY: THE KEY is a software security package for use on an IBM PC or compatible running MS-DOS 2.1 and above. THE KEY allows the user to encrypt or decrypt any file. In addition, THE KEY allows the user to transmit encrypted files over communications links using most binary communications programs. The vendor for this product is PAJAC Systems, Inc.

TRACS 6000: TRACS (Total Response Access and Control System) 6000 involves a small magnetic stripe reader which can be mounted in or near a computer terminal. When a plastic key is inserted into the reader a stream of ASCII data is read from the key and used to verify authorization for access to the terminal. Up to 6000 keys can be used for each stripe reader. The TRACS 6000 Access Control and Alarm Monitoring Terminal can be used to supervise a network of terminals which contain magnetic stripe readers. The vendor for the TRACS 6000 system is Del Norte Technology, Inc.

COMMENTS

In addition to the miscellaneous computer security products mentioned previously, gathered as the result of the *Commerce Business Daily* RFI, there are numerous other miscellaneous products which could enhance computer security. These products include devices for palmprint, speaker, and hand-geometry recognition, keystroke dynamics, and signature verification. An example of each follows:

- **Palmprint Recognition:** The **PG2000**. This vendor for this device is Palmguard, Inc.

- **Speaker Recognition:** The **Conversant 1 Voice System**. The vendor for this product is AT&T Conversant Systems.

- **Keystroke Dynamics: Signature Lock**. This product is provided by Electronic Signature Lock Corporation.

- **Hand Geometry: Identimat ID-2000**. The vendor for this device is Stellar Systems.

- **Signature Verification: Confirma Pen and Tablet:** These devices are manufactured by the Confirma Technology Corporation.

Many of the products described in this section of this paper could be used to improve computer security in workstation environments. This is particularly important for personal computers which might be used for access to classified information.

REFERENCES

1. Department of Defense, "Security Requirements for Automatic Data Processing (ADP) Systems," DOD Directive 5200.28, revised April 1978.

2. Department of Defense, "Computer Security Evaluation Center," DOD Directive 5215.1, October 1982.

3. National Computer Security Center, "Department of Defense Trusted Computer Security Evaluation Criteria," DOD 5200.28-STD, December 1985.

4. National Computer Security Center, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria," July 1987.

5. National Computer Security Center, "Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," CSC-STD-003-85, 25 June 1985.

6. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-85/001.

7. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-85/003.

8. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-86/003.

9. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-86/004.

10. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-86/007.

11. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-87/003.

12. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-84/002.

13. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-85/002.

REFERENCES (Continued)

14. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-84/001.

15. Hale, M.W., "Status of Trusted Database Management System Interpretations," Proceedings of the Tenth National Computer Security Conference, September 1987, p. 340.

16. Air Force Studies Board, *Multilevel Data Management Security*, Committee on Multilevel Data Management Security, National Academy Press, 1983.

17. Graubart, Richard D., "The Integrity-Lock Approach to Secure Database Management," 1984 IEEE Symposium on Security and Protection, Oakland, California.

18. *SIGNAL*, Volume 42, Number 3, November 1987, pp. 5-6.

19. Neugent, William, "Security Guards: Issues and Approaches," U.S. Army Information Systems Engineering Command: Strategies 1987, Alexandria, Virginia.

20. *Commerce Business Daily*, 21 February 1986.

21. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-87/001.

22. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-86/002.

23. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-86/001.

24. The NCSC Serial Number for this product was unavailable at this writing.

25. The NCSC Serial Number for this product was unavailable at this writing.

26. The NCSC Serial Number for this product was unavailable at this writing.

27. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-86/006.

REFERENCES (Concluded)

28. The NCSC Serial Number for this product was unavailable at this writing.

29. National Computer Security Center, "Evaluated Products List for Trusted Computer Systems," Serial: CSC-EPL-SUM-86/005.

APPENDIX A

VENDOR ADDRESSES

- AT&T Conversant Systems, 6200 E. Broad St., Columbus, OH 43213.
- Codercard, 16812 Red Hill, Irvine, CA 92714.
- Computer Security Corporation, 2400 W. Devon Ave., Chicago, IL 60659.
- Confirma Technology Corporation, 333 Ravenswood Ave., Menlo Park, CA 94025.
- CypherMaster, Inc., 4401 Atlantic Avenue, Long Beach, CA 90807-9990.
- Davison Electronics, Inc., 900 North Lehigh St., Baltimore, MD 21205.
- DEL NORTE Technology, Inc., 1100 Pamela Dr., Euless, TX 76040.
- Delta Data Systems Corporation, 1765 Business Center Drive, Reston, VA 22090.
- Digital Dispatch, Inc., 1580 Rice Creek Road, Minneapolis, MN 55432.
- Electronic Signature Lock Corporation, 1311 Ulloa St., San Francisco, CA 94116.
- Enigma Logic, Inc., 2151 Salvio St., Concord, CA 94520.
- Fingermatrix, Inc., 30 Virginia Road, N. White Plains, NY 10603.
- Fischer Innis Systems Corporation, 4175 Merchantile Avenue, Naples, FL 33942.

- Gordian Systems, Inc., 3512 West Bayshore Road, Palo Alto, CA 94303.
- Identix Inc., 2452 Watson Court, Palo Alto, CA 94303.
- PAJAC Systems, Inc., 114 Waltham Street, Lexington, MA 02173.
- Palmguard, Inc., 10260 SW Nimbus Ave., Tigard, OR 97223.
- Security Dynamics, Inc., 15 Dwight St., Boston, MA 02118.
- Spectrum Mfg., Inc., 25 Science Park, New Haven, CT 06511.
- Stellar Systems, 231 Charcot Ave., San Jose, CA 95131.